6712-01

This document is scheduled to be published in the Federal Register on 05/03/2022 and available online at **federalregister.gov/d/2022-09203**, and on **govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 20

[GN Docket No. 13-111; FCC 21-82; FR ID 84137]

Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities

AGENCY: Federal Communications Commission.

ACTION: Final rule; announcement of effective date.

SUMMARY: In this document, the Commission announces that the Office of Management and Budget (OMB) has approved the information collection requirements under OMB Control Number 3060-1299 associated with the Commission's rules adopted in the *Second Report and Order*, FCC 21-82, governing the disabling of contraband wireless devices detected in correctional facilities upon satisfaction of certain criteria, and the advance notice of certain wireless provider network changes to promote and maintain contraband interdiction system effectiveness, and that compliance with these rules is now required. This document is consistent with the *Second Report and Order*, which states that the Commission will publish a document in the **Federal Register** announcing the effective date for these revised rule sections and revise the rules accordingly.

DATES: Instruction 3 amending 47 CFR 20.23 by adding paragraphs (b) through (d), in the final rule published at 86 FR 44635 on August 13, 2021, is effective **[INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

FOR FURTHER INFORMATION CONTACT: Cathy Williams, Office of the Managing Director, Federal Communications Commission, at (202) 418-2918 or Cathy.Williams@fcc.gov.

SUPPLEMENTARY INFORMATION: This document announces that OMB approved the information collection requirements in 47 CFR 20.23 on February 3, 2022. This rule section was adopted in the *Second Report and Order*, FCC 21-82. The Commission publishes this document as an announcement of the immediate effective date for these revised rules.

SYNOPSIS

As required by the Paperwork Reduction Act of 1995 (44 U.S.C. 3507), the Commission is notifying the public that it received final OMB approval on February 3, 2022, for the information collection requirements contained in 47 CFR 20.23. Under 5 CFR part 1320, an agency may not conduct or sponsor a collection of information unless it displays a current, valid OMB Control Number.

No person shall be subject to any penalty for failing to comply with a collection of information subject to the Paperwork Reduction Act that does not display a current, valid OMB Control Number. The OMB Control Number for the information collection requirements in 47 CFR 20.23 is 3060-1299.

The foregoing notice is required by the Paperwork Reduction Act of 1995, Pub. L. 104-13, October 1, 1995, and 44 U.S.C. 3507.

The total annual reporting burdens and costs for the respondents are as follows:

OMB Control Number: 3060-1299.

OMB Approval Date: February 3, 2022.

OMB Expiration Date: February 28, 2025.

Title: Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d), Contraband wireless devices in correctional facilities.

Form Number: N/A

Respondents: Business or other for-profit entities, and state, local or tribal governments.

Estimated Number of Respondents and Responses: 531 respondents and 16,389 responses.

Estimated Time per Response: 1 hour – 10 hours.

Frequency of Response: One-time application and self-certification response, one-time DCFO authorization request response, on occasion qualifying request response, on occasion reversal response, recordkeeping requirement, third party notification requirement.

Obligation to Respond: Required to obtain or retain benefits. Statutory authority for the currently approved information collection is contained in sections 1, 2, 4(i), 4(j), 301, 302, 303, 307, 308, 309, 310, and 332 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 154(j), 301, 302a, 303, 307, 308, 309, 310, and 332.

Estimated Total Annual Burden: 142,568 hours.

Total Annual Cost: No costs.

Needs and Uses: On July 13, 2021, the Commission released a Second Report and Order and Second Further Notice of Proposed Rulemaking, Promoting Technological Solutions to Combat Contraband Wireless Devices in Correctional Facilities, GN Docket No. 13-111, in which the Commission took further steps to facilitate the deployment and viability of technological solutions used to combat contraband wireless devices in correctional facilities. In the Second Report and Order, the Commission adopted a framework requiring the disabling of contraband wireless devices detected in correctional facilities upon satisfaction of certain criteria. The Commission further addressed issues involving oversight, wireless provider liability, and treatment of 911 calls. Finally, the Commission adopted rules requiring advance notice of certain wireless provider network changes to promote and maintain contraband interdiction system effectiveness.

In establishing rules requiring wireless providers to disable contraband wireless devices in correctional facilities and adopting a framework to enable designated correctional facility officials (DCFOs) relying on an authorized Contraband Interdiction System (CIS) to submit qualifying requests to wireless providers to disable contraband wireless devices in qualifying correctional facilities, the Commission found that a rules-based process will provide a valuable additional tool for departments of corrections to address contraband wireless device use. The framework includes a two-phase authorization process: (1) CIS applicants will submit applications to the Wireless Telecommunications Bureau (Bureau) describing the legal and technical qualifications of the systems; and (2) CIS applicants will perform on-site testing of approved CISs at individual correctional facilities and file a self-certification with the Commission. After both phases are complete, DCFOs will be authorized to submit qualifying requests to wireless providers to disable contraband devices using approved CISs at each correctional facility. In addition, the Commission adopted rules requiring wireless providers to notify certain types of CIS operators of major technical changes to ensure that CIS effectiveness is maintained. The Commission found that these rules will provide law enforcement with the

tools necessary to disable contraband wireless devices, which, in turn, will help combat the serious threats posed by the illegal use of such devices.

The new information collection in 47 CFR 20.23(b)(1) regarding the application to obtain new CIS certification will be used by the Bureau to determine whether to certify a system and ensure that the systems are designed to support operational readiness and minimize the risk of disabling a non-contraband device, and ensure, to the greatest extent possible, that only devices that are in fact contraband will be identified for disabling. Bureau certification will also enable targeted industry review of solutions by allowing interested stakeholders to provide feedback on the application for certification, including the proposed test plan.

The new collections in 47 CFR 20.23(b)(3) include the requirement that the CIS operator must file with the Bureau a self-certification that complies with paragraph (b)(3)(ii) of section 20.23, confirming that the testing at that specific correctional facility is complete and successful, and the CIS operator must serve notice of the testing on all relevant wireless providers prior to testing and provide such wireless providers a reasonable opportunity to participate in the tests. Self-certification will help the Bureau to ensure that qualifying requests identify contraband wireless devices accurately and in accordance with legal requirements. In addition to being used by the Bureau, the self-certification will be relied upon by the DCFO in conjunction with qualifying requests for disabling at a particular correctional facility. The serving of notice to the wireless providers will give them awareness and an opportunity to participate in the process.

The new information collections in 47 CFR 20.23(b)(4) afford wireless providers an opportunity to object to the certification filing made after individual site-testing is complete, while requiring objections to be served on the DCFO and the CIS operator. Section 20.23(b)(5) requires that CIS operators retest and recertify their systems at least every three years and comply with the same requirements as for initial self-certification. This requirement will enable the Bureau to ensure the ongoing accuracy and reliability of a given CIS at a particular facility. Section 20.23(b)(7) requires that a CIS operator retain records for at least five years and provide them upon request to the Bureau, which will support the Bureau's efforts to identify issues with

CIS operations, resolve interference issues, and resolve complaints related to misidentification of contraband devices.

The new collections in 47 CFR 20.23(c)(1)-(2) include the requirement that individuals that seek to be recognized on the Commission's DCFO list must send a letter to the Contraband Ombudsperson in order for the Commission to approve that person for the qualified DCFO list and provide certainty to wireless providers that disabling requests are made by duly authorized individuals. Qualifying requests that include the required information will be used by wireless carriers to prevent use of contraband devices on their network and on other wireless provider networks.

The new collections in 47 CFR 20.23(c)(3) and (c)(3)(iii)-(iv) provide that, upon receiving a disabling request from a DCFO, the wireless provider must verify the request, may conduct customer outreach, either reject or grant the request and must notify the DCFO whether it is accepting or rejecting the request. This process ensures that a wireless provider responds to a DCFO within a reasonable timeframe—while giving the provider an opportunity to determine if there is an error—and to give the DCFO time to respond quickly if the request has been rejected. The wireless provider may contact the customer of record to notify them of the disabling and involve them in the process.

The new collections in 47 CFR 20.23(c)(4) provide that a wireless provider may reverse a disabled device where it determines that the device was erroneously identified as contraband, and the wireless provider must notify the DCFO of the reversal. The wireless provider may choose to involve the DCFO in the review and reversal process. The DCFO must also provide notice to the Contraband Ombudsperson of the number of erroneously disabled devices. This process ensures the integrity of the contraband device disabling process by giving the wireless provider the opportunity to reverse a disabled device—with the ability to extend review to the DCFO—and by creating safeguards to make sure that the process is efficient and reliable.

The new collections in 47 CFR 20.23(d) regarding notification from CMRS licensees to MAS operators of technical changes to their network are required so that MAS operators are given sufficient time to make necessary adjustments to maintain the effectiveness of their

interdiction systems. In order to ensure that issues regarding notification to solutions providers of more frequent, localized wireless provider network changes are appropriately considered, CMRS licensees and MAS operators must negotiate in good faith to reach an agreement for notification for those types of network adjustments not covered by the notice requirement. CMRS licensees must provide notice of technical changes associated with an emergency immediately after the exigency to ensure that MAS operators continue to be notified of network changes that could impact MAS effectiveness.

FEDERAL COMMUNICATIONS COMMISSION.

Marlene Dortch,
Secretary.

[FR Doc. 2022-09203 Filed: 5/2/2022 8:45 am; Publication Date: 5/3/2022]